

Justin M. Baxter, Oregon State Bar ID Number 992178
BAXTER & BAXTER, LLP
8835 S.W. Canyon Lane, Suite 130
Portland, Oregon 97225
Telephone: (503) 297-9031
justin@baxterlaw.com

Ari Brown (*Pro Hac Vice*)
RHODES LEGAL GROUP
918 South Horton St., Suite 901
Seattle, WA 98134
Telephone: (206) 412-9320
abrownesq@gmail.com

John Heenan (*Pro Hac Vice*)
HEENAN & COOK
1631 Zimmerman Trail
Billings, MT 59102
Telephone: (406) 839-9091
john@lawmontana.com

Attorneys for Plaintiffs

**IN THE UNITED STATE DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION**

**RICHARD SMITH; WASHINGTON
FEDERAL BANK.** on behalf of themselves
and all others similarly situated,

Plaintiffs,

v.

KAYE-SMITH ENTERPRISES, INC.,

Defendant.

NO. 3:22-CV-01499-AR

**FIRST AMENDED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY

Plaintiffs Richard Smith, and Washington Federal Bank (“WaFd”) individually and on behalf of all other similarly situated (“Class Members”), bring this Complaint against Defendant

Kaye-Smith Enterprises, Inc. (“Kaye-Smith”), and allege the following based on personal knowledge as to their own actions, based on his counsel’s investigations, and upon information and belief as to all other matters as follows:

I. INTRODUCTION

1. Plaintiffs bring this action against Kaye-Smith for its failure to protect and properly secure sensitive personal and financial information including names, Social Security numbers, addresses, phone numbers, dates of birth, financial account numbers, and/or credit scores (collectively “personally identifiable information” or “PII”) belonging to them or to their customers,¹ and for its failure to timely advise Plaintiffs and others that their own and their clients’ PII had been compromised. Plaintiff, Richard Smith seeks to represent a “Consumer Class” made up of consumers who’s PII had been compromised. Plaintiff WaFd seeks to represent a “Business Class” made up of Kaye-Smith’s business clients who relied on Kaye-Smith to safeguard its own customers’ PII and suffered business losses when it failed to do so.

2. Kaye-Smith, is a vendor that generates monthly account statements for various institutional clients including WaFd and Boeing Employees’ Credit Union (“BECU”). Kaye-Smith informed its clients that an unauthorized actor breached Kaye-Smith’s computer network, thereby gaining access to the PII with which its institutional clients entrusted it (the “Data Breach”). Kaye-Smith determined that during the Data Breach, one or more unauthorized actors gained access to the PII of Plaintiffs and over 800,000 Class Members, that included, but was not limited to, their

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver’s license number, financial account number).

names, addresses, account numbers, credit information, and “masked” Social Security Numbers. These Class Members have already suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out of pocket expenses, loss of value of their time incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in value of their PII.

3. Kaye-Smith waited at least six weeks and possibly significantly longer before notifying governmental entities and individuals whose PII may have been compromised. Plaintiff, Richard Smith received notice of the Data Breach from BECU.

4. The customers of WaFd and of Kaye-Smith’s other clients entrust them with an extensive amount of their PII. WaFd contracted with Kaye-Smith to provide the service of printing and distributing periodic statements. Kaye-Smith understands the importance of protecting such information and specifically undertakes the burden of protecting the PII in its contract with WaFd and its other clients. Kaye Smith had explicit contractual obligations to each of the Business Class members to safeguard the PII entrusted to it.

5. Defendant breached the terms of its standard form contract into which it entered with each Business Class Member.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff and the Consumer Class members’ PII, Kaye-Smith assumed legal and equitable duties to those individuals.

7. The exposed PII of Plaintiffs and Consumer Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Consumer Class Members face a lifetime risk of identity theft.

8. This PII was compromised due to Kaye-Smith’s negligent and/or careless acts and

omissions and their respective failure to protect PII of Plaintiff and Consumer Class Members and to maintain adequate safeguards.

9. Plaintiff and Consumer Class Members suffered and will continue to suffer injury due to Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

10. Plaintiff Richard Smith was a resident of Pierce County, Washington at times relevant to this action and has recently relocated to Pima County, Arizona.

11. Plaintiff WaFd is a Washington chartered bank headquartered in Seattle, Washington.

12. Defendant Kaye-Smith is a for-profit corporation organized under the laws of Oregon, with its principal office located in Renton, Washington and one of three primary offices located in Portland, Oregon.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C.

§ 1332(d)(2), because (a) there are 100 or more Class members, (b) Plaintiffs are citizens of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

14. This Court has personal jurisdiction over Defendant because it is organized under the laws of the State of Oregon, maintains an office in this District and does business in Oregon and/or transacted business in Oregon.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Kaye-Smith's place of business is located in this District.

IV. FACTUAL ALLEGATIONS

Background

16. Kaye-Smith's clients collected and stored some of Plaintiff Smith's and Class Members' most sensitive and confidential information, including Social Security numbers, home addresses, phone numbers, dates of birth, financial account numbers, and other PII, which is static, does not change, and can be used to commit myriad financial crimes.

17. WaFd's members entrust it with an extensive amount of their PII. WaFd in turn, entrusted Kaye-Smith with this PII.

18. Kaye-Smith contracted with WaFd and other business clients, to provide vendor services. In the course of providing those services, Kaye-Smith obtained the PII of Plaintiff and Consumer Class Members. Kaye-Smith retains this information on computer hardware and asserts that it understands the importance of protecting such information.

19. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Consumer Class Members' PII, Kaye-Smith assumed legal and equitable duties to those individuals.

20. Kaye-Smith was aware, or should reasonably have been aware, that the PII it agreed to obtain and safeguard is highly sensitive and of significant value to those who would use it for wrongful purposes.

21. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”³

22. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have PII, “they can drain your bank account, run up your credit cards, open new utility accounts, or get treatment on your medical insurance.”

23. Identity thieves can use PII such as the PII of Plaintiff Smith and Consumer Class Members which Defendant failed to secure, to perpetrate other varieties of crimes that harm victims. A “cyber black market” exists in which criminals openly post and sell PII. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff Smith and Consumer Class Members face a lifetime risk of identity theft.

24. Professionals tasked with combatting cybercriminals know that PII has real monetary value in part because criminals continue their efforts to obtain this data. In other

² 17 C.F.R. § 248.201 (2013).

³ *Id.*

words, if any additional breach of sensitive data did not have incremental value to criminals, a reduction in criminal efforts to obtain such data over time would occur. However, just the opposite has occurred, with data breaches rising

25. This PII was compromised due to Kaye-Smith's negligent and/or careless acts and omissions and the failure to adequately protect PII of Plaintiff and Consumer Class Members.

26. Kaye-Smith bills itself as "a leader in the execution and management of business-critical communications." It touts on its website its "three pillars of security" which "allow us to meet and exceed the most stringent requirements associated with data communications, and materials handling for the financial, medical, biotech and insurance industries." As such, Kaye-Smith is well aware of the need to protect PII.

27. Kaye-Smith assumed a non-delegable duty to protect the PII of Plaintiff and the Consumer Class members.

28. Ransomware is a malware designed by cybercriminals to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cybercriminals place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom. Ransomware has quickly become the most prominent and visible type of malware. Kaye-Smith, at all relevant times, knew or should have known that cyber criminals seek out PII, especially through ransomware.

29. Best practices such as cyber awareness training, continuous data backups, patching, and encryption all exist to prevent ransomware attacks by cybercriminals.

The Data Breach

30. On July 29, 2022, Plaintiff Smith received a letter from BECU dated July 25, 2022, entitled “Important Privacy Protection Notification.” that stated:

At BECU, we value your business and respect the privacy of your information, which is why we are writing to let you know about a vendor network security incident that involves your personal information. We encourage you to read this entire letter because it contains important information concerning the security of your account(s) at BECU. It also includes our offer to provide you with one year of credit monitoring protection at no cost to you unless otherwise required by local law. We take the protection of your information very seriously and are contacting you directly to explain the circumstances of the incident. To learn more, visit becu.org/vendor-incident.

What happened?

On June 6, 2022, BECU was informed that its printing vendor had experienced a network security incident. At that time, BECU took immediate measures to protect member information by suspending services with the vendor. After the incident occurred, the vendor indicated that some BECU member information in process at the time of the incident was potentially involved. On July 5, 2022, we were able to determine that your personal information was involved after an independent forensics firm had analyzed the compromised data. We sincerely apologize for any inconvenience or concern this incident may cause.

What information was involved?

The information involved may have included your name, address, account number(s), credit score, and Social Security number.

What we are doing.

The security of accounts and the protection of personal information – for you and all our members – are top priorities at BECU. We are committed to ensuring the security of your personal information. BECU worked with the vendor and a forensics firm before resuming services to improve the security of the vendor’s environment as well as its effectiveness at preventing and detecting future cybersecurity incidents.

We understand you may have concerns, so we have secured Equifax Credit Watch™ Gold to provide you credit monitoring protection at no cost for one (1) year unless otherwise required by local law.

31. On July 23, BECU posted a notice on its website, which it updated on July 25.⁴

What Happened

On June 6, BECU was informed that our third-party printing vendor had experienced a network security incident that impacted their printing and notification services for our members and involved unauthorized access to certain data of some members. At that time, BECU took immediate measures to protect member information by suspending services with the vendor.

The vendor engaged a third-party forensics firm to investigate the incident to identify what data was accessed and to restore operations. We continued to communicate with the vendor regularly throughout the investigation to monitor and understand implications for members.

On July 5, we were able to determine what information was accessed after the third-party forensics firm analyzed the incident and provided their findings. We are satisfied with the steps the vendor has undertaken and have resumed regular operations.

As of July 25, we have begun notifying impacted members with letters sent via USPS mail. As shared in the notification, members with questions or concerns about this incident can reach out to our partner Epiq Corporate Services at 877-390-2571, Monday-Friday, 7 a.m.-7 p.m. Pacific Time. We take the security of our members' accounts and personal information very seriously and sincerely apologize for any inconvenience or concern this incident may cause.

As BECU resumed services with the vendor, members are receiving their delayed statements and correspondence. While all monthly statements will be available by the end of July, we expect that some delivery delays will continue for several weeks as we return to regular production schedules. Members may also have received some statements and correspondence out of order. We recognize the inconvenience and we appreciate your patience while we work to get caught up.

Who Is Affected?

We understand you may have concerns and we take these matters very seriously. We began mailing letters on July 25 to members whose data was impacted by the incident. Members with questions or concerns on this incident can reach out to our partner Epiq Corporate Services at 877-390-

⁴ See <https://www.becu.org/news/2022/important-notice-about-vendor-incident-and-delayed-statements>

2571. We encourage you to refer to the FAQ below for steps to be proactive with your account security.

Our Commitment

Securing and protecting our members' privacy and sensitive information remains our highest priority. We continually monitor accounts for suspicious and unauthorized activity. We are communicating to all members whose data was impacted by the incident and provided an offer for free credit monitoring protection for reassurance and increased security.

When we were informed of the incident, BECU immediately suspended services with the vendor. As a result of this service interruption, delivery of monthly statements and other correspondence to members was delayed. We worked to provide alternative options during this time and implemented back-up processes for communication to members, as much as possible. We apologize for any inconvenience you may have experienced.

32. BECU stated in its website notice and in the letter it sent to Plaintiff that a vendor (later identified as Kaye-Smith) with whom BECU had contracted to provide printing services, allowed unauthorized access to the members' PII that it received from BECU. Kaye-Smith was subject to a ransomware attack that included the PII of Plaintiff and other Consumer Class Members as well as the PII of customers of WaFd and Kaye-Smith's other business clients.

33. Plaintiffs and both the Business Class and Consumer Class Members retain a vested interest in ensuring that PII in Kaye-Smith's possession remains protected.

34. Plaintiff and Consumer Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Consumer Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Consumer Class Members.

35. Kaye-Smith did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and for

Consumer Class Members, causing their PII to be exposed.

Kaye-Smith is Entrusted with Consumer Class Members' PII.

36. WaFd and Business Class Members acquired, collected, and stored Plaintiff's and Consumer Class Members' PII that they collect at the time each member opens an account as a condition of providing services to their customers.

37. WaFd and each Business Class Member contracted with Kaye-Smith to provide vendor services by entering into a standard form contract that Kaye-Smith drafted. Under the terms of the contract, Kaye-Smith specifically acknowledged that it would be receiving PII related to WaFd and each Business Class Member's customers (i.e.: Consumer Class Members) and assumed legal and equitable duties to protect the PII from disclosure.

38. Plaintiff and Consumer Class Members have taken reasonable steps to maintain the confidentiality of their PII. They relied on the Business Class Members and their vendor, Kaye-Smith to keep their PII confidential and securely maintained, to use this information for business purposes only, to adequately maintain adequate procedures and safeguards to keep the PII confidential, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches.

39. Kaye-Smith could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Consumer Class Members.

40. Kaye-Smith's negligence in safeguarding the PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

41. Despite the prevalence of public announcements of data breach and data security compromises, Kaye-Smith failed to take appropriate steps to protect the PII entrusted to it from being compromised.

42. The ramifications of Defendant's failure to keep secure Plaintiffs' and Consumer Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

43. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁵ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.⁶ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.⁷

44. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding

⁵ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed August 1, 2022).

⁶ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed August 1, 2022).

⁷ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed August 1, 2022).

payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.⁸

45. Changing or canceling a stolen Social Security number is a difficult task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted because an individual must show evidence of actual, ongoing fraud activity to obtain a new Social Security number.

46. Moreover, a new Social Security number may not be an effective remedy to an identity theft. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”⁹

47. Based on the foregoing, the information compromised in Kaye-Smith’s Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and it is difficult, if not impossible, to change.

48. This data that Kaye-Smith failed to safeguard demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are

⁸ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed August 1, 2022).

⁹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed August 1, 2022).

worth more than 10x on the black market.”¹⁰

49. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

50. The PII of Consumer Class Members was likely taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from Kaye-Smith’s Data Breach may not come to light for years.

51. There may also be a time lag between when harm occurs versus when it is discovered and also between the time PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹¹

52. At all relevant times, Kaye-Smith knew, or reasonably should have known, the importance of safeguarding Plaintiff’s and Consumer Class Members’ PII and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Consumer Class Members.

53. Plaintiff and Consumer Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

¹⁰ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed August 1, 2022).

¹¹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/products/gao-07-737> (last accessed August 1, 2022).

54. One year of identity monitoring is inadequate to protect Plaintiff and Consumer Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

55. The injuries to Plaintiff and Consumer Class Members were directly and proximately caused by Kaye-Smith's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Richard Smith's Experience

56. Richard Smith is a retired Kitsap County, Washington Deputy Sheriff.

57. In approximately 2009 Mr. Smith opened both a personal checking account and a business account at a BECU branch in Tacoma, Washington. He had transferred to BECU from Bank of America after becoming disillusioned with what he felt were incessant and unjustified fees Bank of America was charging and wanted to bank at a smaller and more consumer-friendly institution. He was, however, wary of banking at a small credit union that may not have sufficiently sophisticated safeguards to protect his sensitive information. He chose BECU in part, based on BECU's assurances regarding its level of sophistication and its commitment to keeping sensitive information secure—including when sharing information with its vendors.

58. As a condition of opening accounts at BECU, Mr. Smith was required to provide detailed PII that included his address, telephone number, email address, Social Security number, date of birth, business tax identification number, and driver's license number. BECU stored and/or shared some of Mr. Smith's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII resulting in the exposure of Mr. Smith's PII during the Data Breach.

59. After learning of the Data Breach, Mr. Smith purchased a subscription to an identity theft protection service and credit monitoring service.

60. In addition, as a result of learning of the Data Breach, Mr. Smith has spent, and is continuing to spend, time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, at least two hours exploring credit monitoring and identity theft insurance options, and self-monitoring his financial accounts. This time has been lost and cannot be recaptured.

61. Mr. Smith has been careful about sharing his PII. He has not knowingly transmitted unencrypted PII over the internet or any other unsecured source, and stores documents containing his PII in a secure location or destroys the documents.

62. Mr. Smith suffered actual injury in the form of money spent on credit monitoring and identity theft protection as well as damages to, and diminution of the value of his PII—a form of intangible property that Mr. Smith entrusted to BECU as a customer, that was in turn entrusted to Defendant, and which was compromised in and as a result of the Data Breach.

63. Mr. Smith has also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, distress, and increased concerns for the loss of his privacy.

64. Mr. Smith has suffered additional injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and Social Security number being placed in the hands of unauthorized parties and possibly criminals.

65. Mr. Smith has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

66. Plaintiffs brings this action as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class and Subclass, under CR 23(a) and (b)3.

67. The proposed Classes are defined as:

Consumer Class

All persons residing in the United States whose personally identifiable information Kaye-Smith obtained, stored and/or shared and which was exposed to an unauthorized party as the result of the data breach referenced in BECU's correspondence to Plaintiffs Smith dated July 25, 2022.

Business Class

Any and all businesses or entities that had a business relationship with Kaye-Smith, including Kaye-Smith's clients, and whether such relationship was by contract or not, and that were affected by the Data Security Incident, excluding those who have resolved their claims against Kaye-Smith prior to October 19, 2023.

Plaintiffs reserve the right to modify, change, or expand the Class definitions, including proposing subclasses, based on discovery and further investigation.

68. Excluded from the Classes are Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

69. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their respective claims on a class-wide basis using the same evidence that would be used to prove those elements in individual actions alleging the same claims.

70. Numerosity and Ascertainability. The members of the Classes are so numerous that a joinder of all members would be impracticable. Kaye-Smith holds itself out as a leading Northwest marketing execution and supply chain company, serving corporate clients across a wide range of industries. On information and belief, the PII of over 800,000 individuals was compromised during Kaye-Smith's Data Breach. The Class Members are readily ascertainable from information and records in the possession, custody, or control of Kaye-Smith. Notice of this action can readily be provided to the Class. The Business Class, in turn, is comprised of in excess of 20 members class who entered into contracts with Kaye-Smith.

71. Commonality and Predominance (CR 23(a)(2) and CR 23(b)(3)). There are numerous questions of law and fact common to Plaintiffs and members of the Class. Those common questions of law or fact predominate over questions that may affect only individual Class members. The common issues arising from Kaye-Smith's conduct predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. The questions of law and fact common to Plaintiffs and members of the Class include, among others, the following:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Consumer Class Members;
- b. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Consumer Class Members;
- c. When Defendant actually learned of the Data Breach;

- d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII or the PII of their clients had been compromised;
- e. Whether Defendant failed to implement and maintain sufficient security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- f. Whether Defendant adequately addressed and ensured that the vulnerabilities that permitted the Data Breach to occur had been fixed;
- g. Whether Plaintiff and the Consumer Class were intended third party beneficiaries of the contract between Kaye-Smith and Business Class Members.
- h. Whether Kaye-Smith breached implied duties to the Consumer Class Members that were created by its contracts with the Business Class Members.
- i. The contractual obligations Kaye-Smith owed to Plaintiff WaFd and Business Class Members;
- j. Whether Kaye-Smith is liable to Business Class Members for damages due to disclosure of the Confidential Information by unauthorized third parties;
- k. Whether Kaye-Smith breached its contractual obligations to Business Class Members;
- l. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced because of the Data Breach.

72. Typicality. Plaintiff Smith's claims are typical of the claims of all Consumer Class Members in that the PII of the representative Plaintiff, like that of all Class Members, was compromised in the Data Breach. The evidence and legal theories regarding Kaye-Smith's alleged failings are substantially the same for Plaintiffs and all the Class Members. Plaintiff WaFd's claims are typical of the claims of all Business Class Members in that Kaye-Smith's contractual obligations to each Business Class Member to safeguard the confidential information entrusted to it was substantially the same and was compromised as a result of the same Data Breach, and WaFd suffered damages similar to the Business Class including but not limited to lost time and out-of-pocket expenses associated with notice and remediation.

73. Adequacy. Plaintiffs will fairly and adequately protect the respective interests of each Class. Plaintiffs have retained capable and competent attorneys who have significant experience in complex and class action litigation, including consumer rights litigation. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of each Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to or that conflict with those of the Class.

74. Superiority. Plaintiffs and Class Members have suffered and will continue to suffer harm and damages as a result of Defendants' conduct. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitive. Class treatment is superior to multiple individual suits or piecemeal litigation because it conserves judicial resources, promotes consistency and efficiency of adjudication, provides a forum for small claimants, and deters illegal activities. There will be no significant difficulty in the management of this case as a class action.

VI. CHOICE OF LAW

75. This action arises from a Data Breach of PII collected from Plaintiff and Class Members at branches located in the State of Washington. It further arises from the performance of

a contracts that were created and performed in the State of Washington and from the safeguarding of PII that was transferred to Defendant from computer servers located in Washington and, on information and belief, was stored in Washington.

76. Under applicable conflicts of laws principles regarding both common law contracts and torts, the substantive law of the state of Washington governs the claims in this action.

VII. CLAIMS

First Cause of Action

Negligence

(on behalf of Plaintiff Smith and the Consumer Class)

77. Plaintiffs incorporate the above allegations as if fully set forth here.

78. In the course of providing vendor services as part of its business and for its own profit, Kaye-Smith obtained and accepted possession of the PII of Plaintiffs and Consumer Class Members including their names, Social Security numbers, bank account numbers, home addresses, phone numbers, and dates of birth

79. Kaye-Smith has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Consumer Class could and would suffer if the PII were wrongfully disclosed. Kaye-Smith knew or should have known that Plaintiff's and the Consumer Class' sensitive PII was an attractive target to cyber thieves.

80. Kaye-Smith knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Consumer Class involved an unreasonable risk of harm to Plaintiff and the Consumer Class, even if the harm occurred through the criminal acts of a third party. Kaye-Smith uniquely knows the importance of protecting PII from cyber criminals.

81. Kaye-Smith had a non-delegable duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or

disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing both its security protocols to ensure that the PII of Plaintiff and the Class that was in its possession was adequately secured and protected.

82. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

83. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting, storing, and sharing the PII of Plaintiff and the Consumer Class, along with the critical importance of ensuring adequate security of that PII at all times.

84. Defendant had the ability to sufficiently guard against data breaches. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Consumer Class. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII in the face of increased risk of theft.

85. Defendant breached the duty to exercise reasonable care in protecting Plaintiff's and the Consumer Class Members' PII by failing to take reasonable security measures, and by ensuring that its vendors took reasonable security measures, to safeguard and adequately secure the PII from unauthorized access.

86. Under RCW 19.255.010(1), Kaye-Smith also owed a duty to timely disclose to Plaintiff and to the Consumer Class Members that their PII had been, or was reasonably believed to have been, compromised. Timely disclosure was necessary so that Plaintiff and the Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their

social security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) routinely monitor loan data and public records; and (6) take other steps to protect themselves and recover from identity theft.

87. Kaye-Smith breached its duty to timely disclose the Data Breach to Plaintiff and the Consumer Class Members. After learning of the Data Breach, Kaye-Smith unnecessarily delayed notifying Plaintiff and Class Members in a sufficiently conspicuous manner.

88. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

89. There is a causal connection between Defendant's failure to implement and/or maintain security measures to protect the PII of Plaintiff and the Consumer Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Consumer Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

90. As a direct and proximate result of Defendant's failings, Plaintiff and the Consumer Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

91. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Consumer Class suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Second Cause of Action
Breach of Implied Contract
(On Behalf of Plaintiff Smith and the Consumer Class)

92. Plaintiffs incorporate the above allegations as if fully set forth here.

93. Plaintiff Smith and all other Consumer Class Members provided their personal information, including names, Social Security numbers, home addresses, phone numbers, dates of birth, and other personal information, as a condition of receiving services from Business Class Members, which Plaintiff and each Consumer Class Member provided.

94. Each Business Class Member contracted with Kaye-Smith for services for which Plaintiff and the Consumer Class were the intended beneficiaries, and under which Kaye-Smith has undertaken duties to act for the benefit of Plaintiff Smith and the Consumer Class.

95. As part of its contractual performance, Kaye-Smith accepted possession of the PII of Plaintiff and the Consumer Class and agreed to safeguard and protect such information, to keep

such information secure and confidential, and to timely and accurately notify Plaintiff and the Consumer Class Members if their data had been breached and compromised or stolen.

96. Kaye-Smith breached the contractual duties it undertook for the benefit of Plaintiff and the Consumer Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the Data Breach.

97. As a direct and proximate result of Kaye-Smith's above-described breach, Plaintiff and the Consumer Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

Third Cause of Action
Breach of Contract
(on behalf of WaFd and the Business Class)

98. Plaintiffs incorporate the above allegations as if fully set forth here.

99. Plaintiff, WaFd and each Business Class member entered into a written agreement with Kaye-Smith that constitutes a binding contract.

100. Under the terms of the contract, Kaye-Smith was obligated to hold the PII entrusted to it in strict confidence using a sufficient degree of care to prevent the unauthorized disclosure to any third party.

101. Under the terms of the contract, Kaye-Smith was obligated to establish data security policies and procedures to ensure the security and confidentiality of the PII entrusted to it, to protect it against any anticipated threats or hazards to its security, and to protect against unauthorized access to the PII.

102. Under the terms of the contract, Kaye-Smith was required to promptly notify WaFd and each Business Class Member following the discovery of any actual breach of security to the information systems it maintains and to take prompt remedial action to mitigate the effects of any breach of security.

103. Kaye-Smith breached the terms of its contracts with each of the Business Class Members by failing to comply with the above referenced obligations.

104. As a direct and proximate result of Kaye-Smith's breaches of its contractual obligations, Plaintiff WaFd and the Business Class Members suffered damages in amounts to be proven at trial and are entitled to recovery of such damages.

Fourth Cause of Action
Washington Consumer Protection Act
RCW 19.86, et seq.
(On Behalf of Plaintiff Smith and the Consumer Class)

105. Plaintiffs incorporate the above allegations as if fully set forth here.

106. Kaye-Smith is a person within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

107. Plaintiff Smith and the Consumer Class Members are "persons" within the meaning of RCW 19.86.010(1).

108. Kaye-Smith engaged in unfair or deceptive acts or practices in the conduct of its business by the conduct set forth above. These unfair or deceptive acts or practices include: failing

to adequately secure Plaintiff's and the Consumer Class Members' sensitive personal information from disclosure to unauthorized third parties or for improper purposes; enabling the disclosure of personal and sensitive facts about Plaintiff and the Class Members; enabling the disclosure of personal and sensitive facts about Plaintiff and the Class members without their informed, voluntary, affirmative, and clear consent; and omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiff's and the Class Members' sensitive personal information.

109. Kaye-Smith's systematic acts or practices are unfair because they (1) caused substantial financial injury to Plaintiff and the Consumer Class Members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

110. Kaye-Smith's systematic acts or practices are unfair because the acts or practices are immoral, unethical, oppressive, and/or unscrupulous.

111. Kaye-Smith's systematic acts deceptive as they were and are capable of deceiving a substantial portion of the public.

112. Kaye-Smith's unfair or deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of RCW 19.86.010 and RCW 19.86.020 and are ongoing and/or have a substantial likelihood of being repeated.

113. Kaye-Smith's unfair or deceptive acts or practices impact the public interest.

114. As a direct and proximate result of Kaye-Smith's unfair or deceptive acts or practices, Plaintiff and the Consumer Class Members have suffered injury in fact.

115. As a result of Kaye-Smith's conduct, Plaintiff and the Consumer Class members have suffered actual damages including from fraud and identity theft, time and expenses related to

monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm.

116. Plaintiff and the Consumer Class members are therefore entitled to legal relief against Kaye-Smith's, including recovery of nominal damages, actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

117. Plaintiff and the Consumer Class members are also entitled to injunctive relief in the form of an order prohibiting Kaye-Smith's from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for an order:

- a. Certifying this case as a class action, appointing Plaintiff Smith as Class Representative of the Consumer Class, appointing Plaintiff WaFd as Class Representative of the Business Class, and appointing Plaintiffs' counsel to represent the Classes;
- b. Entering judgment for Plaintiffs and the Classes;
- c. Awarding Plaintiffs and Class Members monetary relief;
- d. Ordering appropriate injunctive relief;
- e. Awarding pre and post judgment interest as prescribed by law;
- f. Awarding reasonable attorneys' fees and costs as permitted by law; and
- g. Granting such further relief as may be just and proper.

Plaintiffs further demands trial by jury.

DATED this ___ day of June, 2024.

Respectfully submitted,

s/ Justin M. Baxter

Justin M. Baxter, Oregon State Bar ID Number 992178

Email: justin@baxterlaw.com

BAXTER & BAXTER, LLP

8835 S.W. Canyon Lane, Suite 130

Portland, Oregon 97225

Telephone (503) 297-9031

Facsimile (503) 291-9172

Ari Y. Brown, *pro hac vice*

RHODES LEGAL GROUP, PLLC

918 South Horton Street, Suite 901

Seattle, Washington 98134

206-708-7852

Fax 206-906-9230

John Heenan, *pro hac vice*

HEENAN & COOK

Email: john@lawmontana.com

1631 Zimmerman Trail

Billings, Montana 59102

Telephone: (406) 839-9081

Attorneys for Plaintiffs